The Honorable John C. Coughenour

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

REBECCA COUSINEAU, individually on her own behalf and on behalf of all others similarly situated, Plaintiff, v. MICROSOFT CORPORATION, a Delaware corporation, Defendant.	No. 11-cv-01438-JCC MICROSOFT'S MOTION FOR SUMMARY JUDGMENT ***Note on Motion Calendar:*** January 17, 2014 **Oral Argument Requested**

Davis Wright Tremaine LLP
LAW OFFICES
Suite 2200 · 1201 Third Avenue
Seattle, Washington 98101-3045
(206) 622-3150 · Fax: (206) 757-7700

TABLE OF CONTENTS

Davis Wright Tremaine LLP
LAW OFFICES
Suite 2200 · 1201 Third Avenue
Seattle, Washington 98101-3045
(206) 622-3150 · Fax: (206) 757-7700

TABLE OF AUTHORITIES

Page(s)

Federal Cases

Davis Wright Tremaine LLP
LAW OFFICES
Suite 2200 · 1201 Third Avenue
Seattle, Washington 98101-3045
(206) 622-3150 · Fax: (206) 757-7700

Davis Wright Tremaine LLP
LAW OFFICES
Suite 2200 · 1201 Third Avenue
Seattle, Washington 98101-3045
(206) 622-3150 · Fax: (206) 757-7700

Federal Statutes

Rules

Davis Wright Tremaine LLP
LAW OFFICES
Suite 2200 · 1201 Third Avenue
Seattle, Washington 98101-3045
(206) 622-3150 · Fax: (206) 757-7700

Other Authorities

Davis Wright Tremaine LLP
LAW OFFICES
Suite 2200 · 1201 Third Avenue
Seattle, Washington 98101-3045
(206) 622-3150 · Fax: (206) 757-7700

I. INTRODUCTION

Rebecca Cousineau sued Microsoft because she thought it was collecting location information from her Samsung phone—which used Microsoft's Windows Phone 7 operating system—and "tracking" her whereabouts without her consent. Cousineau Dep. (3/13) 13:11-20; 23:10-24:7 (Dkt. 94, Ex. 9). But as Ms. Cousineau learned in discovery, Microsoft ***never*** used location data to track any Windows Phone 7 user. Her class certification motion [Dkt. 69] thus abandons her tracking claim, instead asserting a new Stored Communications Act ("SCA") theory. Because her new tack lacks any legal or factual basis, Microsoft asks for summary judgment.

Ms. Cousineau's current SCA theory attacks functions occurring entirely on her phone, without data transmission to Microsoft (or anyone else). According to Ms. Cousineau, Microsoft is liable under the SCA because a bug in the Windows Phone 7 Camera application caused her phone to request location information stored in her phone's random access memory ("RAM") every time she launched the Camera, even though she allegedly hit "cancel" when asked whether she wanted to allow it to use her location. Class Cert Mot. [Dkt. 69] 8:2-5. In other words, Ms. Cousineau's theory no longer rests on Microsoft gaining unauthorized access to or receiving information stored on her phone. Rather, she argues Microsoft is liable because one Windows Phone 7 software component (i.e., the Camera application) requested information stored elsewhere on the phone (i.e., RAM), without her permission. Ms. Cousineau urged the Court to certify a class to pursue this peculiar theory of liability, "without evaluating the theory itself." *Id*. 21:2-3.

On this motion, Microsoft asks the Court to "evaluat[e] the theory itself"—and to reject it. In claiming Microsoft faces SCA liability based on the behavior of her phone's software, Ms. Cousineau ignores undisputed facts established through discovery and seeks to stretch the SCA beyond recognition. The Court should grant summary judgment for any one of four reasons:

First, Microsoft did not and cannot "access" the location information stored in RAM on Ms. Cousineau's phone. Her new theory rests on the untenable premise that regardless of whether any location information was transmitted to Microsoft's servers (or off her phone at all), Microsoft violated the SCA because her phone's Camera application, a software component, could call for

Davis Wright Tremaine LLP
LAW OFFICES
Suite 2200 · 1201 Third Avenue
Seattle, Washington 98101-3045
(206) 622-3150 · Fax: (206) 757-7700

location data stored in RAM on her phone after she allegedly denied the Camera application permission to do so. But the SCA imposes no liability for software unexpectedly accessing electronic communications—unless the software facilitates the ***defendant's*** access to those communications. Here, because the Camera application's call to RAM did not allow Microsoft to access Ms. Cousineau's electronic communications, the SCA does not apply.

Second, Ms. Cousineau expressly permitted other Windows Phone 7 applications to use her location information—just not the Camera application. As a result, Ms. Cousineau's claim challenges an alleged misuse of location information (by the Camera application) she authorized Microsoft to access for other purposes. But the SCA penalizes only unauthorized ***access*** to data—not unauthorized ***use*** of data a defendant was permitted to access. Because Ms. Cousineau gave Microsoft authority to access her location information, the SCA does not reach her claim.

Third, the SCA prohibits unauthorized access only to a "facility through which an electronic communications service is provided." 18 U.S.C. § 2701(a). In denying Microsoft's Motion to Dismiss, this Court declined to hold as a matter of law that a mobile device can ***never*** be a facility under the SCA. Order [Dkt. 38] 10:20-11-12. Since then, discovery established Ms. Cousineau's phone does not function as a "facility," and several courts (including one in this district) have held similar devices enabling users to take advantage of similar services are not "facilities." A contrary reading would give service providers (rather than users) the right to authorize third-party access to personal devices, an illogical result Congress clearly did not intend.

Fourth, when Windows Phone 7's location framework software requests location information in RAM, it does not "access" a "communication" in "electronic storage," as the SCA defines those terms. The SCA defines "electronic storage" as (a) "temporary, intermediate storage … incidental to the electronic transmission" of a communication or (b) backup storage of the communication. 18 U.S.C. § 2510(17). But the location data stored in RAM on a Windows Phone 7 device has reached its final destination. Because the information is not in "intermediate" storage "incidental to . . . transmission" or stored for backup purposes, even unauthorized access to that information (which did not occur in any event) falls outside the SCA.

Davis Wright Tremaine LLP
LAW OFFICES
Suite 2200 · 1201 Third Avenue
Seattle, Washington 98101-3045
(206) 622-3150 · Fax: (206) 757-7700

II. FACTUAL BACKGROUND

This case involves location services, a feature Microsoft makes available to Windows Phone 7 users. Microsoft's Opposition to Motion for Class Certification [Dkt. 90] ("Class Opp.") explains the background to the dispute, which revolves around unexpected behavior involving the use of location information by the Camera application (and ***only*** the Camera application) in the Windows Phone 7 operating system. The anomalous behavior occurred between October 2010 and August 2011, and Microsoft took immediate steps to notify users and correct the behavior when it learned of it. *See* Class Opp. 3:19-4:3, 7:11-24. The anomaly occurred only because of a desire to improve the user experience by making location information available to users of the Windows Phone 7 Camera promptly upon request. *See* Lydick Decl. [Dkt. 92] ¶ 2. And discovery has established Microsoft ***never*** used any data transmitted as a result of the anomaly to track users or intrude on their privacy. Class Opp. 6:20-7:9.

Microsoft will not repeat its previous discussion of how the unexpected behavior arose or what it did in response. Instead, this Motion focuses on how Microsoft's location service actually functions and explains why Ms. Cousineau has no viable claim under the SCA.

A. Location Services on Windows Phone 7

Most modern smartphones offer location services, which make possible useful features, such as mapping and navigation. Del Amo Casado Decl. [Dkt. 91] ¶ 3. Windows Phone 7 includes several software applications (or "apps") that incorporate location information to provide services to the user. *Id*. For example, the Maps app can use location information to give the user directions from his or her current location to a desired destination. *Id*. The Search app can use location information to deliver search results tailored to the user's current location. *Id*. And the Camera app can use location information to "tag" the pictures a user takes with the place where they were taken. *Id*.

Applications incorporating location services must obtain location information by making a request (or "call") to a software component of the Windows Phone 7 operating system called "the location framework." Class Cert. Mot. [Dkt. 69] 5:12-14. A Windows Phone 7 device generally

Davis Wright Tremaine LLP
LAW OFFICES
Suite 2200 · 1201 Third Avenue
Seattle, Washington 98101-3045
(206) 622-3150 · Fax: (206) 757-7700

allows an application to call the location framework only if the user enables location services in the device's settings. Del Amo Casado Decl. [Dkt. 91] ¶ 4. (The one exception to this general rule is the Find My Phone application, which can access location even when the master location switch is turned off. *Id.*) When an application is permitted to make such a request, the call for location "goes from one software component loaded on the phone (the application) to another software component loaded on the phone (the location framework)." *Id.* ¶ 5. The location framework then applies logic to return location information to the application. *Id.*

In general, the location framework logic handles a location request in three ways: first, it can contact other software components on the device and obtain a GPS (i.e., global positioning system) fix for the phone's location; second, it can request an approximate location from Microsoft, through a cloud-based location service known as "Orion"; and third, it can request location data already stored in the phone's RAM as a result of a previous request to Orion. *Id.* ¶ 6. Ms. Cousineau has never made any allegation implicating the resolution of location through a GPS fix. This Motion therefore focuses on the other two methods of resolving location.

Both of the other methods, i.e., using Microsoft's Orion location service and using location data stored in RAM on the phone, involve the process of inferring location based on nearby observed "beacons," a term referring to WiFi access points (such as wireless internet routers used in homes and businesses) and mobile phone cell towers. Del Amo Casado Decl. [Dkt. 91] ¶ 8. When it receives a location request, the location framework determines what beacons are nearby and tries to find location information (i.e., latitude and longitude information) about those beacons. *Id.* The Orion service has location information on beacons all around the world. *Id.* ¶ 9. After the location framework collects beacon information, it may transmit identifiers for those beacons to Orion; if Orion has latitude and longitude information for the beacons, it returns the information to the location framework, which relays it to the requesting application. *Id.* Orion also returns to the phone multiple "tiles" (essentially pieces of a map of beacons) containing location information for all known beacons in the vicinity. *Id.* The Windows Phone 7 software

Davis Wright Tremaine LLP
LAW OFFICES
Suite 2200 · 1201 Third Avenue
Seattle, Washington 98101-3045
(206) 622-3150 · Fax: (206) 757-7700

stores the tiles in the phone's memory, where the location framework can retrieve them to resolve future location requests efficiently ***without*** communicating with Microsoft. *Id.*

Because "[t]he quickest and most efficient way to obtain a location fix is to resolve location from information stored in memory on the phone, without sending or receiving information from off the device," Microsoft designed its software so the location framework tries to resolve location requests using data already on the phone. Del Amo Casado Decl. [Dkt. 91] ¶ 10. Before it sends any beacon information to Orion, the location framework first looks to tiles stored in RAM on the phone itself, to determine if the tiles contain location information for the beacons in the vicinity of the phone. *Id.* Thus, if a user is in an area covered by tiles already stored in RAM, "location requests will be resolved on the device without transmitting any data to Microsoft's location service. The location framework sends a location request, with associated data, to Microsoft's servers ***only*** if the tiles stored in RAM cannot resolve the user's location." *Id.* Ms. Cousineau and her expert witness admit Microsoft designed the Windows Phone 7 software to resolve location efficiently ***on the device***, if possible: "Upon receipt of [a location] request, Location Framework would always look first to the device's RAM for temporarily stored location information. (Del Amo Casado Tr. at 100:3 -17; Snead Rpt. at 13)." Class Cert. Mot. [Dkt. 69] 6:11-13. Put another way, Microsoft designed Windows Phone 7 so location framework can "resolve a User's location (including when responding to location requests from Camera) ***without any external communications*** or network connectivity." *Id.* 14:17-20 (citing Del Amo Casado Tr. 84:17-25, 100:3-101:13, 105:20-106:2) (emphasis added).

Tiles stay on the phone for roughly ten days before the Windows Phone software 7 discards them as stale. Del Amo Casado Decl. [Dkt. 91] ¶ 14. "Once tiles are unloaded from memory, they disappear. The information contained on the tiles is not communicated back to Microsoft or anywhere else, and the device has no record of unloaded tiles." *Id.*; *see also* Snead Dep. (Rummage SJ Decl. Ex. 1) 70:17-71:7 (confirming "once [a tile is] overwritten or replaced by another tile, it's just lost").

Davis Wright Tremaine LLP
LAW OFFICES
Suite 2200 · 1201 Third Avenue
Seattle, Washington 98101-3045
(206) 622-3150 · Fax: (206) 757-7700

B. Ms. Cousineau's New Claim

Ms. Cousineau no longer argues ***Microsoft*** accessed information stored on her Windows Phone 7 without her consent. Rather, Ms. Cousineau now contends Microsoft "design[ed] ***the*** . . . ***Camera*** to *always* access RAM regardless of user authorization" and claims Microsoft therefore "violated Cousineau's and the class members' rights under the SCA." Class Cert. Reply [Dkt. 97] 3:17-19 (first emphasis added). In other words, Ms. Cousineau asks the Court to award statutory damages because one Microsoft application (the Camera) overrode her instructions when it requested information stored in her phone's RAM—even though Ms. Cousineau allowed other Microsoft applications to retrieve and use ***the same location information***. *See* Class Cert. Mot. [Dkt. 69] 18:11-15 (referring to Ms. Cousineau's "documented past usage of location services for other purposes (e.g., to obtain directions and local restaurant and hotel recommendations)"); Cousineau Dep. (3/13) 47:22-49:4 (Dkt. 72-23, Ex. M) (discussing use of location services through mapping and search applications); Cousineau Decl. [Dkt. 72-26] ¶¶ 3-6 (describing specific instances of using location). Further, Ms. Cousineau seeks those statutory damages even though, ***after*** filing suit, she continued to use the Camera app—even while believing "that taking pictures would continue to transmit tracking information or location information." Cousineau Dep. (3/13) 51:15-18 (Dkt. 94, Ex. 9).

As explained below, this software glitch does not provide Ms. Cousineau with a legal basis to pursue windfall statutory damages under a statute intended to punish criminal hacking.

III. ARGUMENT

The Court should grant summary judgment when "there is no genuine issue as to any material fact and … the movant is entitled to a judgment as a matter of law." Fed. R. Civ. P. 56(a). To avoid summary judgment, the nonmovant (here, Ms. Cousineau) must come forward with "specific facts showing that there is a *genuine issue for trial*." *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 587 (1986) (emphasis in original). When "the record taken as a whole could not lead a rational trier of fact to find for the non-moving party, there is no genuine issue for trial." *Id.* (citation omitted). Once the moving party has shown the absence of a disputed issue of fact, it is entitled to summary judgment if the non-moving party fails to present, by

Davis Wright Tremaine LLP
LAW OFFICES
Suite 2200 · 1201 Third Avenue
Seattle, Washington 98101-3045
(206) 622-3150 · Fax: (206) 757-7700

affidavits, depositions, answers to interrogatories, or admissions on file, "specific facts showing that there is a genuine issue for trial." *Celotex Corp. v. Catrett*, 477 U.S. 317, 324 (1986). "[T]he moving party may simply point to the absence of evidence to support the nonmoving party's case." *In re Brazier Forest Prod. Inc.*, 921 F.2d 221, 223 (9th Cir. 1990). At that point, the non-movant may not rest on allegations in the pleadings. *Kaiser Cement Corp. v. Fischbach & Moore, Inc.*, 793 F.2d 1100, 1103-04 (9th Cir. 1986). Conclusory statements, speculation, personal beliefs, and unsupported assertions will not suffice to withstand summary judgment, and a court will not "presume" "missing facts." *Lujan v. Nat'l Wildlife Fed'n*, 497 U.S. 871, 888-89 (1990).

Here, Microsoft moves for summary judgment on Ms. Cousineau's only remaining claim, which she asserts under the SCA. Congress passed the SCA "aim[ing] at computer hackers" who access communications while stored with certain kinds of communications providers. *Konop v. Haw. Airlines, Inc.*, 302 F.3d 868, 890 (9th Cir. 2002) (citations omitted). Section 2701 of the SCA (on which Cousineau relies) does not provide a basis for liability against Microsoft because it (a) imposes liability only on persons (or entities) who access information without authorization, which Microsoft does ***not*** do when the Camera application calls RAM to resolve location; (b) does not prohibit alleged misuse of information a defendant had the right to access for some purposes; (c) addresses only unauthorized access to "facilities through which an electronic communication service is provided," a term that nearly every court has held excludes mobile devices such as Ms. Cousineau's Windows Phone 7 device; and (d) protects only communications in intermediate storage incidental to transmission or for backup purposes, which does not describe the location information ("tiles") stored in RAM on Ms. Cousineau's phone. *See* 18 U.S.C. §§ 2701(c)(1), (2).

A. Microsoft Did Not Violate the SCA When the Location Framework on Ms. Cousineau's Device Requested Location Information from RAM.

As explained by her expert witness, Ms. Cousineau's claim rests on the premise "the code that Microsoft wrote," ***not*** Microsoft itself, "is accessing RAM" on her Samsung phone. Snead Dep. 36:15-16 (Rummage SJ Decl. Ex. 1). In other words, Ms. Cousineau argues Microsoft violated the SCA because "Location Framework, a piece of software[,] accesses the RAM," and "Microsoft wrote th[at] software"— even though Microsoft itself does not access or receive any

Davis Wright Tremaine LLP
LAW OFFICES
Suite 2200 · 1201 Third Avenue
Seattle, Washington 98101-3045
(206) 622-3150 · Fax: (206) 757-7700

information stored in the RAM. *Id*. 38:11-22; *see also id*. 111:20-23. According to Ms. Cousineau's expert, her SCA theory "doesn't necessarily mean that information is transmitted to Microsoft or anywhere else off the device," *id*. 113:7-14; instead, her theory depends on processes taking place entirely within the operating system of the phone itself. In other words, these internal processes do not result in the transmission of data or enable Microsoft to learn of or track Ms. Cousineau's whereabouts. Del Amo Casado Decl. [Dkt. 91] ¶ 21(c). "Microsoft cannot access location information stored in RAM; indeed, Microsoft does not even have a way to know when location framework accesses RAM to resolve a location request." *Id*. ¶ 21(d).

Based on these facts, Ms. Cousineau argues "by designing the [Windows Phone 7] Camera to *always* access RAM regardless of user authorization, Microsoft violated Cousineau's and the class members' rights under the SCA." Class Cert. Reply [Dkt. 97] 3:17-19. In other words, she says Microsoft violated the SCA because (a) it designed the Windows Phone 7 software, and (b) the software allowed the Camera application to continue to access location information stored in RAM. Nothing in the words of the SCA or the cases interpreting it suggests software behavior of that nature (which was unintended, caused no harm, and was promptly fixed) gives rise to the software designer's liability under the statute.

Congress passed the SCA "to protect [against] potential intrusions on individual privacy." *Garcia v. City of Laredo*, 702 F.3d 788, 791 (5th Cir. 2012), *cert. denied*, 133 S. Ct. 2859 (2013). The statute accomplishes this goal by imposing liability on

> ***whoever***—
>
> (1) intentionally ***accesses*** without authorization a facility through which an electronic communication service is provided; or
>
> (2) intentionally exceeds an authorization to ***access*** that facility;
>
> and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system …

18 U.S.C. §§ 2701(a) (emphasis added). The SCA allows any person "aggrieved" by a "knowing or intentional" violation of this provision to recover not less than $1,000 per violation from "the ***person or entity*** … which engaged in that violation." 18 U.S.C. § 2707(a), (c) (emphasis added).

Davis Wright Tremaine LLP
LAW OFFICES
Suite 2200 · 1201 Third Avenue
Seattle, Washington 98101-3045
(206) 622-3150 · Fax: (206) 757-7700

To begin with, Ms. Cousineau has no basis to argue Microsoft "accessed" her Samsung Windows Phone 7 device—or "obtain[ed], alter[ed], or prevent[ed] . . . access to" any communications stored on the phone—merely because the Camera application made a call to the location framework, which in turn retrieved information from the phone's RAM. Instead, the undisputed evidence shows "Microsoft cannot access location information stored in RAM"; in fact, it "does not even have a way to know when location framework accesses RAM to resolve a location request." Del Amo Casado Decl. [Dkt. 91] ¶ 21(d). Microsoft knows of no authority suggesting a defendant can be liable under the SCA where the defendant itself does not ***actually*** access a facility and thereby obtain, alter, or prevent access to electronic communications the facility stores. Because even Ms. Cousineau's expert agrees only the Camera app (not Microsoft) accessed or used the information in question, she has no SCA claim.

Further, the SCA provides for civil liability only where a "person or entity" violates the statute. 18 U.S.C. § 2707(a). As the SCA's legislative history explains, Section 2701 "addresses the growing problem of unauthorized ***persons*** deliberately gaining access to, and sometimes tampering with, electronic or wire communications that are not intended to be available to the public." S. Rep. No. 541, 99th Cong., 2nd Sess. 1986, 1986 U.S.C.C.A.N. 3555, 3589, 1986 WL 31929, *35 (Oct. 17, 1986) (emphasis added). "[T]he sort of trespasses to which the Stored Communications Act applies are those in which the ***trespasser*** gains access to information to which he is not entitled to see." *Educ. Testing Serv. v. Stanley H. Kaplan, Educ. Center, Ltd.*, 965 F. Supp. 731, 740 (D. Md. 1997) (emphasis added); *see also In re Am. Airlines, Inc., Privacy Litig.*, 370 F. Supp. 2d 552, 558-59 (N.D. Tex. 2005); *Cardinal Health 414, Inc. v. Adams,* 582 F. Supp. 2d 967, 976 (M.D. Tenn. 2008). Because Ms. Cousineau cannot show that any "person or entity" accessed information stored in RAM (instead, she relies on the fact the Camera application, did so), she cannot recover under the SCA.

Ms. Cousineau argues "Microsoft cannot evade liability by shifting the blame to its software," and she tells the Court "it is well-settled that a corporation can act by way of software or code." Class Cert. Reply [Dkt. 97] 5:1, 6:23. But the two cases on which Ms. Cousineau relies

Davis Wright Tremaine LLP
LAW OFFICES
Suite 2200 · 1201 Third Avenue
Seattle, Washington 98101-3045
(206) 622-3150 · Fax: (206) 757-7700

support Microsoft: both involve defendants using software to access and obtain a plaintiff's electronic communications. In *Miller v. Meyers,* 766 F. Supp. 2d 919, 923 (W.D. Ark. 2011), for example, the defendant "admitted to using a keylogger program to obtain Plaintiff's passwords" and "then used those passwords to access Plaintiff's email account without authorization." And in *Harris v. comScore, Inc.*, 292 F.R.D. 579, 582-83 (N.D. Ill. 2013), the defendant used software to "intercept[] phone numbers, social security numbers, user names, passwords, bank account numbers, credit card numbers, and other demographic information," and then sold "the data collected from the consumer's computer." In stark contrast, when the Camera app requested information from RAM on Ms. Cousineau's phone, Microsoft neither accessed the device nor received information from the device—as Ms. Cousineau's expert concedes. Snead Dep. 38:11-22, 111:20-23, 113:7-14 (Rummage SJ Decl. Ex. 1).

Nothing in the record indicates Microsoft "gain[ed] access to information . . . [it was] not entitled to see," *Educ. Testing Service*, 965 F. Supp. at 740, when the phone's location framework retrieved information from RAM in connection with the Camera's location request. That fact, without more, entitles Microsoft to summary judgment on Ms. Cousineau's SCA claim.[1]

B. Ms. Cousineau Concedes She Authorized Microsoft to Access Location Information on Her Phone, Which Disposes of Her SCA Claim.

Ms. Cousineau's claim rests on the theory Microsoft violated the SCA when the Camera app erroneously called for location information stored in the phone's RAM—even while she authorized other Microsoft apps to access the same information. By leaving the master location service switch "on" in her device settings, Ms. Cousineau permitted Microsoft applications (such as Maps) to access location information stored in RAM. *See* Class Cert. Mot. [Dkt. 69] 18:11-15

[1] Nor could Ms. Cousineau survive summary judgment on the "tracking" theory she abandoned in her class certification motion. In addition to her failure to satisfy the other elements of her SCA claim (discussed below), that theory fails because Ms. Cousineau cannot carry her burden of showing her Windows Phone 7 software caused her phone to transmit location data to Microsoft without her consent. "In many common circumstances, a location request will not result in any communication to Microsoft's Orion location service, either to resolve the location request or to crowd source data that might be obtained as a result of the location request." Del Amo Casado Decl. [Dkt. 91] ¶ 20; *see also* Class. Opp. [Dkt. 90] 13:21-25 (citing Del Amo Casado Decl. ¶¶10-12). Ms. Cousineau has no evidence she ever launched her Camera application in circumstances possibly leading to the transmission of location data without her consent, and her inability to come forward with evidence on the point would justify judgment in Microsoft's favor—if Ms. Cousineau were still pursuing the claim. *See Celotex*, 477 U.S. at 322 (summary judgment proper if party fails to "make a showing sufficient to establish the existence of an element essential to that party's case, and on which that party will bear the burden of proof at trial"); *Weinstock v. Columbia Univ.*, 224 F.3d 33, 41 (2nd Cir. 2000) (at summary judgment, "[t]he time has come … 'to put up or shut up'") (citation omitted).

Davis Wright Tremaine LLP
LAW OFFICES
Suite 2200 · 1201 Third Avenue
Seattle, Washington 98101-3045
(206) 622-3150 · Fax: (206) 757-7700

(referring to her "documented past usage of location services for other purposes (e.g., to obtain directions and local restaurant and hotel recommendations)"); Cousineau Dep. (3/13) 47:22-49:4 (Dkt. 72-23, Ex. M) (discussing use of location services with Microsoft's Maps and Internet Explorer applications). She has no evidence the Camera app accessed location tiles she had not previously authorized other Microsoft applications (such as Maps or Internet Explorer) to access. Thus, even accepting the unfounded premise Microsoft accessed location information in RAM when the Camera app made a request to the location framework, Ms. Cousineau cannot show Microsoft accessed information it lacked authority to access. Her inability to make that showing means she cannot carry her burden under the SCA, entitling Microsoft to summary judgment.

Ms. Cousineau's theory fails because the SCA forbids unauthorized ***access*** to communications, not unauthorized ***use*** of communications a defendant was authorized to access for some purposes. *E.g.*, *Educ. Testing Serv.*, 965 F. Supp. at 740; *Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda*, 390 F. Supp. 2d 479, 494-99 (D. Md. 2005) (dismissing SCA claim based on defendant's misuse of information to which defendant had authorized access). "Because section 2701 of the ECPA prohibits only unauthorized access and not the misappropriation or disclosure of information, there is no violation of section 2701 for a person with authorized access to the database no matter how malicious or larcenous his intended use of that access. Section 2701 outlaws illegal entry, not larceny." *Sherman & Co. v. Salton Maxim Housewares, Inc.*, 94 F. Supp. 2d 817, 821 (E.D. Mich. 2000). In other words, "the sort of trespasses to which the [SCA] applies are those in which the trespasser gains access to information to which he is not entitled to see, not those in which the trespasser uses the information in an unauthorized way." *Educ. Testing Serv.*, 965 F. Supp. at 740.

In this respect, the SCA is comparable to the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, which contains language similar to Section 2701 and, like the SCA, also is intended to punish hackers.[2] *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1130 (9th Cir.

[2] The most commonly invoked provision of the CFAA provides for liability against anyone who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains … information from any protected computer." 18 U.S.C. § 1030(a)(2).

Davis Wright Tremaine LLP
LAW OFFICES
Suite 2200 · 1201 Third Avenue
Seattle, Washington 98101-3045
(206) 622-3150 · Fax: (206) 757-7700

2009). The Ninth Circuit has held the CFAA's prohibitions against accessing protected computers "without authorization" or "exceeding authorized access" apply ***only*** where a defendant obtains information it was not permitted to access ***for any purpose***. *See United States v. Nosal*, 676 F.3d 854, 864 (9th Cir. 2012) (*en banc*) (Kozinski, C.J.) (if defendant "had permission to access the company database and obtain the information contained within" for certain purposes, misuse of that information did not violate the CFAA); *Brekka*, 581 F.3d at 1135. Where a defendant has permission to access information for ***some*** purposes, no liability attaches because the CFAA is "limited to violations of restrictions on *access* to information, and not restrictions on *use*." *Nosal*, 676 F.3d at 864 (emphasis in original).

Thus, even if the Court were to accept Ms. Cousineau's theory that Microsoft "acts through" the applications on Windows Phone 7 (even though no information is transmitted to its servers), she has no evidence Microsoft retrieved location information stored in RAM in connection with the Camera app that she did not otherwise consent to share through other applications. Ms. Cousineau does not claim Microsoft wrongfully "accessed" location information stored in RAM—she admits Microsoft had authority to access the same location information in RAM when she used Maps, made location-related searches, or otherwise used location services with other Microsoft apps. Rather, Ms. Cousineau's theory is, at most, that Microsoft's programming allowed the Camera app to use location information already stored on her phone against her wishes. But because the SCA does not provide a cause of action for misuse of information, Microsoft is entitled to summary judgment on her claim.

C. Microsoft Did Not Access a "Facility" When the Windows Phone 7 Location Framework Made a Call to RAM on Ms. Cousineau's Phone.

Even if Ms. Cousineau had evidence showing Microsoft gained unauthorized "access" to her communications when her Camera application initiated a call to location framework, she must also show Microsoft did so by accessing a "***facility*** through which an electronic communications service is provided." 18 U.S.C. § 2701(a) (emphasis added). The evidence shows Ms. Cousineau's phone is ***not*** a "facility" under the SCA.

Davis Wright Tremaine LLP
LAW OFFICES
Suite 2200 · 1201 Third Avenue
Seattle, Washington 98101-3045
(206) 622-3150 · Fax: (206) 757-7700

When Microsoft moved for an order certifying for interlocutory review the question whether a mobile device can be a "facility" within the meaning of the SCA, the Court decided the issue was "intertwined with various undeveloped and unresolved factual issues, including the way geolocation information was generated and transmitted to Microsoft, the manner by which Microsoft provided an 'electronic communication service' through the Windows Phone, and whether the users' location data was accessed by Microsoft at a point when it was being held in temporary storage." Order [Dkt. 47] 3:18-23. Now, with those issues resolved through discovery, Microsoft asks the Court to hold Ms. Cousineau's Windows Phone 7 is not a "facility."

To determine whether a Windows Phone 7 device is a "facility through which an electronic service is provided," 18 U.S.C. § 2701(a), the Court must identify the "electronic communications service" at issue. Section 2510(12) defines "electronic communication" to include "any transfer of … data[] or intelligence of any nature transmitted in whole or in part by a … radio … system." Ms. Cousineau alleges transmission of location data to (and from) Microsoft falls within the definition of "electronic communication" in Section 2510(12). *See* Third Amended Compl. [Dkt. 64] ¶¶42, 46. Section 2510(15) in turn defines "electronic communication service" ("ECS") to mean "any service which provides to users thereof the ability to send or receive … electronic communications," including data. Here, the ECS involves the transmission of beacon data from Ms. Cousineau's Samsung phone, running Windows Phone 7, to the Orion service, and the return of location inference data from Orion to the phone. Del Amo Casado Decl. [Dkt. 91] ¶¶ 8, 9. But Orion provides ECS to the Windows Phone 7 device—not vice versa. "The Windows Phone 7 device … functions as the 'client' for location services provided by the GPS satellites and Orion." *Id.* ¶ 19. When the device resolves location, it does so based on data ***received*** from the service; it does not ***provide*** the service itself.

Several courts within the last two years have held that a mobile device is not a "facility" for purposes of the SCA. In *Garcia v. City of Laredo*, 702 F.3d 788, 793 (5th Cir. 2012), *cert. denied*, 133 S. Ct. 2859 (2013), the Fifth Circuit canvassed case law (including cases within this circuit), academic literature, and legislative history before concluding "[a]n individual's personal

Davis Wright Tremaine LLP
LAW OFFICES
Suite 2200 · 1201 Third Avenue
Seattle, Washington 98101-3045
(206) 622-3150 · Fax: (206) 757-7700

cell phone does not *provide* an electronic communication service just because the device *enables* use of electronic communications services." Similarly, in *Shefts v. Petrakis*, 2013 U.S. Dist. LEXIS 17213, *15 (C.D. Ill. 2013), the district court held a Blackberry phone was not a "facility" under the SCA; rather, "[a] Blackberry is merely a device, a miniature computer, that enables a person to use Verizon's text messaging service, not a facility operated by Verizon." And in *Lazette v. Kulmatycki*, 2013 WL 2455937, *5 (N.D. Ohio 2013), the district court concluded "the better, more sensible, and harmonious reading of the SCA is that … a blackberry or cell phone[] is not a 'facility' within §2701(a)(1)."[3] And finally, in *In re iPhone Application Litigation*, 844 F. Supp. 2d 1040, 1058 (N.D. Cal. 2012)—another case involving allegedly unauthorized access to location information—the court dismissed the SCA claim, noting that treating an iPhone as a "facility" would lead to anomalous results under the statute.[4]

In dismissing the SCA claim, the district court in *iPhone* relied on *Crowley v. CyberSource Corp.*, 166 F. Supp. 2d 1263 (N.D. Cal. 2001), which rejected an SCA claim predicated on the characterization of a user's personal computer as a "facility through which an electronic communication service is provided." The court in *Crowley* noted the provider of an electronic communication service can authorize access to any facility through which the service is provided. *Id.* at 1271 (citing 18 U.S.C. § 2701(c)(1)). As a result, if the user's personal computer were a "facility," the SCA would allow the ECS provider (e.g., Comcast or another ISP), and not just the user, to grant third parties access to the PC. "It would … seem odd that the provider of a

[3] Judge Carr, the author of *Lazette*, is co-author of one of the leading electronic communications privacy treatises. *See* Hon. James Carr & Patricia Bellia, Law of Elec. Surveillance (2012).

[4] Many other recent cases—including a recent decision from Judge Leighton—hold the SCA does not reach personal computers. *See, e.g., In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 2013 U.S. Dist. LEXIS 145727, *24 (D. Del. 2013) ("An individual's personal computing device is not 'a facility through which an electronic communication service is provided,' as required under the SCA."); *Roadlink Workforce Solutions LLC v. Malpass*, 2013 U.S. Dist. LEXIS 133786, *10 (W.D. Wash. 2013) (personal computer not a "facility"); *Morgan v. Preston*, 2013 U.S. Dist. LEXIS 159641, *14-17 & n.3 (M.D. Tenn. 2013) (citing cases illustrating "the overwhelming body of law" holding "an individual's personal computer is not a 'facility through which an electronic communication service is provided'"); *see also United States v. Cioni*, 649 F.3d 276, 282 (4th Cir. 2011) (juxtaposing crimes under SCA with similar criminal computer fraud statute: "the two crimes are distinct and different. Section 1030(a)(2)(C) punishes the obtaining of information through the unauthorized access to a ***computer***, whereas § 2701(a) punishes accessing without authority a "***facility*** through which an electronic communication service is provided" and thereby obtaining communications that are "***in electronic storage***.") (emphasis in original); *Thule Towing Sys. LLC v. McNallie*, 2009 WL 2144273, *5-6 (E.D. Mich. 2009) (rejecting SCA claim because personal laptop was not a facility); *Borinski v. Williamson*, 2005 WL 1206872, *11 (N.D. Tex. 2005) (accessing emails on laptop not an SCA violation). Although the Court need not decide whether personal computers can be facilities under the SCA, these cases rely on reasoning applicable with equal or greater force to smart phones.

Davis Wright Tremaine LLP
LAW OFFICES
Suite 2200 · 1201 Third Avenue
Seattle, Washington 98101-3045
(206) 622-3150 · Fax: (206) 757-7700

communication service could grant access to one's home computer to third parties, but that would be the result of Crowley's argument." *Id.*; *see also Roadlink Workforce Solutions LLC v. Malpass,* 2013 U.S. Dist. LEXIS 133786, *10 (W.D. Wash. 2013) (Leighton, J.) (citing *Crowley* and holding personal computer not a "facility").

A "fundamental canon of statutory construction" makes clear "the words of a statute must be read in their context and with a view to their place in the overall statutory scheme." *Davis v. Mich. Dept. of Treasury*, 489 U.S. 803, 809 (1989). A court must interpret a statute "as a symmetrical and coherent regulatory scheme." *Gustafson v. Alloyd Co*., 513 U.S. 561, 569 (1995). As *Crowley* recognizes, the SCA's exemptions would make no sense if "facility" were read to encompass a Windows Phone 7 device: as the provider of location services, *see* Order [Dkt. 38] 11:22-23 ("the Court finds that Microsoft is an ECS provider for the purposes of the SCA"), it would mean ***Microsoft*** could grant access to ***any*** Windows Phone 7 device to ***any*** person, without the user's consent. Nothing would more clearly run counter to the SCA's purposes of protecting the privacy of people's stored electronic communications—"but that would be the result of [the] argument" being advanced by Ms. Cousineau here.[5]

It makes no difference to the analysis that a Windows Phone 7 device enables the use of location services. Users of an ECS by definition require a device allowing them to connect to the service—but that does not make the device a facility used to ***provide*** the service. *Shefts*, 2013 U.S. Dist. LEXIS 17213, *15 ("A Blackberry is merely a device, a miniature computer, that enables a person to use Verizon's text messaging service, not a facility operated by Verizon."); *Freedom Banc Mortg. Servs, Inc. v. O'Harra*, 2012 WL 3862209, *9 (S.D. Ohio 2012) ("[T]he relevant 'facilities' that the SCA is designed to protect are not computers that enable the use of an electronic communication service, but instead are facilities that are operated by electronic communication service providers[.]"). As the district court explained in *In re Pharmatrak Privacy*

[5] Ms. Cousineau cannot escape the absurdity by labeling herself the ECS provider instead of Microsoft: if she were an ECS provider, the SCA would impose on her the duties and responsibilities of a service provider, including obligations to (a) preserve evidence, 18 U.S.C. § 2703(f); (b) assist in electronic surveillance, 18 U.S.C. § 2511(2); and (c) report to the National Center for Missing and Exploited Children, 18 U.S.C. § 2258A. In fact, Congress intended to place those responsibilities only on those who offer an ECS to third parties, not on users.

Davis Wright Tremaine LLP
LAW OFFICES
Suite 2200 · 1201 Third Avenue
Seattle, Washington 98101-3045
(206) 622-3150 · Fax: (206) 757-7700

Litigation, 220 F. Supp. 2d 4, 13 (D. Mass. 2002), *rev'd on other grounds*, 329 F.3d 9 (1st Cir. 2003), it makes no difference that "[p]ersonal computers provide consumers with the opportunity to access the Internet and send or receive electronic communications" and "[w]ithout personal computers, most consumers would not be able to access the Internet or electronic communications"; to become a "facility through which an electronic communication service is provided," a personal computer would need "to perform server-like functions." *Id.*; *see also* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1214-15 (2004) ("While a home computer configured as a mail server could provide ECS in theory, the home computer of an end user is not protected by the SCA.").[6]

Nothing revealed in discovery differentiates Ms. Cousineau's Windows Phone 7 device from the similar devices (such as Blackberries and iPhones) courts regularly hold fall outside the SCA's meaning of a "facility." The SCA "protects users whose electronic communications are in electronic storage with an ISP or other electronic communications facility," *Theofel v. Farey-Jones*, 359 F.3d 1066, 1072-73 (9th Cir. 2003)—not in storage on a user's personal device.

D. Location Information Stored in RAM Fails to Satisfy the SCA's Requirement of Storage "Incidental to" Transmission or for Backup.

Section 2701 of the SCA also requires Ms. Cousineau to prove Microsoft obtained "access to … [an] electronic communication while it [was] in electronic storage." Congress defined "electronic storage" to include only "(A) any temporary, ***intermediate*** storage of a wire or electronic communication ***incidental to the electronic transmission*** thereof; and (B) any ***storage*** of such communication ***by an electronic communication service for purposes of backup*** protection of such communication." 18 U.S.C. § 2510(17) (emphasis added). Ms. Cousineau cannot satisfy either prong of the definition: when her device stored location tiles in RAM, the

[6] Although Professor Kerr is the most oft-cited SCA commentator, others agree the statute does not reach users' devices, such as PCs or cellphones. *See, e.g.,* Hon. James Carr & Patricia Bellia, 1 Law of Elec. Surveillance § 3:76 (2012) (SCA does not "apply where access is to the plaintiff's computer rather than to the facility of an electronic communication service") (citations omitted); *id.* § 4.76 (SCA does not apply to data on a personal hard drive); Carr, *supra*, 2 Law of Elec. Surveillance § 8:35 ("Where access is to the plaintiff's computer rather than to the facility of an electronic communication service, no cause of action arises."); Proskauer on Privacy § 6:3.1, at 6-94 (PLI 2012) (cataloguing decisions; concluding the "better view" is "home computers are not, in the ordinary course of their operation, ECS facilities").

Davis Wright Tremaine LLP
LAW OFFICES
Suite 2200 · 1201 Third Avenue
Seattle, Washington 98101-3045
(206) 622-3150 · Fax: (206) 757-7700

storage was neither "intermediate" and "incidental to the electronic transmission thereof" nor "for purposes of backup."

As Section 2510(17)(A)'s references to "temporary" and "intermediate" storage make clear, the SCA "only protects electronic communications stored 'for a limited time' in the 'middle' of a transmission, i.e., when an electronic communication service temporarily stores a communication while waiting to deliver it." *In re DoubleClick, Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 512 (S.D.N.Y. 2001). "[T]he definition [of electronic storage] … covers a message that is stored in intermediate storage temporarily, after the message is sent by the sender, but before it is retrieved by the intended recipient." *Fraser v. Nationwide Mut. Ins. Co.*, 135 F. Supp. 2d 623, 636 (E.D. Pa. 2001), *aff'd in part, vacated in part on other grounds*, 352 F.3d 107 (3d Cir. 2004). As the Ninth Circuit noted (citing *DoubleClick* and *Fraser*), "[s]everal courts have held that subsection (A) covers e-mail messages stored on an ISP's [or related] server pending delivery to the recipient." *Theofel*, 359 F.3d at 1075. Thus, even ***if*** mobile phones were facilities (and they are not), the data stored on the Windows Phone 7 device after delivery is not in "temporary, intermediate storage … incidental to … electronic transmission." *Hilderman v. Enea TekSci, Inc.*, 551 F. Supp. 2d 1183, 1204-05 (S.D. Cal. 2008) (emails stored on PC after receipt not in "temporary, intermediate storage"); *In re Toys R Us, Inc. Privacy Litig.*, 2001 U.S. Dist. LEXIS 16947, *10-12 (N.D. Cal. 2001) (cookies on PCs not in "temporary, intermediate storage").

In the right circumstances, accessing electronic communications while in RAM ***may*** satisfy the SCA definition of electronic storage, because "RAM is 'a computer component in which data and computer programs can be temporarily stored.'" *In re Toys R Us Privacy Litig.*, 2001 WL 34517252, *12 (quoting *MAI Systems Corp. v. Peak Computer, Inc.*, 991 F.2d 511, 519 (9th Cir. 1993)). But the SCA definition ***also*** requires storage of the electronic communication be both "intermediate" and "incidental to the electronic transmission thereof." 18 U.S.C. § 2510(17). To satisfy the SCA, access therefore must occur "when an electronic communication service temporarily stores a communication while ***waiting to deliver it***." *In re DoubleClick*, 154 F. Supp. 2d at 512 (emphasis added).

Davis Wright Tremaine LLP
LAW OFFICES
Suite 2200 · 1201 Third Avenue
Seattle, Washington 98101-3045
(206) 622-3150 · Fax: (206) 757-7700

The Windows Phone 7 location framework's retrieval of tiles stored in RAM does ***not*** occur while those tiles are being transmitted from Microsoft's Orion service or while the tiles are awaiting delivery elsewhere. Rather, the tiles reside in RAM as a resource the software can access to resolve location requests. Del Amo Casado Decl. [Dkt. 91] ¶ 9 ("Windows Phone 7 then stores the tiles on the phone, where they will be available to resolve future location requests efficiently without taking the time, power, and bandwidth necessary to communicate with Orion."). Further, the storage of tiles on the Windows Phone 7 fails to satisfy the equally important requirement of "intermediate" storage: the tiles in RAM have reached their destination, and even Ms. Cousineau's expert witness acknowledged the tiles "don't go someplace else after they are done." Snead Dep. 71:5-7 (Rummage SJ Decl. Ex. 1). After ten days, or as new tiles need the space, the tiles vanish. Del Amo Casado Decl. [Dkt. 91] ¶ 14. The software therefore does ***not*** access the tiles while in "temporary, intermediate storage … incidental to the electronic transmission thereof," as the SCA requires. *See Shefts,* 2013 U.S. Dist. LEXIS 17213, *16 ("by the time the messages were on the Blackberry … their transmission was complete, and so the storage could not be 'temporary, intermediate storage … incidental' to it"); *In re DoubleClick*, 154 F. Supp. 2d at 512 (dismissing SCA claim where storage of cookies did not occur as "an 'intermediate' step in their transmission to another addressee").

Nor does the Camera application access tiles while they are stored "by an electronic communication service for purposes of backup protection." 18 U.S.C. § 2510(17)(B). Ms. Cousineau has never claimed the tiles in her phone's RAM functioned as backup. In any event, the definition of "electronic storage" contemplates storage ***by the service provider*** for backup, and no evidence suggests Microsoft downloaded tiles to Ms. Cousineau's phone to back up location information in the Orion database. *See Garcia*, 702 F.3d at 793 (text message and photos stored on phone not stored by ECS provider for backup); *Shefts,* 2013 U.S. Dist. LEXIS 17213, *16-17 (dismissing SCA claim because ECS provider did not use Blackberry "for backup protection"). To the contrary, the uncontroverted testimony establishes the Windows Phone 7 software downloads location tiles to facilitate a user's access to location services—because "[t]he quickest

Davis Wright Tremaine LLP
LAW OFFICES
Suite 2200 · 1201 Third Avenue
Seattle, Washington 98101-3045
(206) 622-3150 · Fax: (206) 757-7700

and most efficient way to obtain a location fix is to resolve location from information stored in memory on the phone, without sending or receiving information from off the device." Del Amo Casado Decl. [Dkt. 91] ¶ 10; Snead Report [Dkt. 72-4] 6:21-7:4.

In sum, when the phone's location framework accesses information from tiles stored in RAM, it does not access a communication in "electronic storage," as Section 2510(17) defines that term. This provides yet another independently sufficient basis for summary judgment.

IV. CONCLUSION

Microsoft respectfully asks the Court to grant summary judgment dismissing Ms. Cousineau's SCA claim—the only claim remaining in the case.[7]

DATED this 5th day of December, 2013.

DAVIS WRIGHT TREMAINE LLP
Attorneys for Defendant Microsoft Corporation

By */s/ Stephen M. Rummage*

Stephen M. Rummage, WSBA #11168
Fred B. Burnside, WSBA #32491
Zana Bugaighis, WSBA #43614
1201 Third Avenue, Suite 2200
Seattle, Washington 98101-3045
Telephone: (206) 622-3150, Fax: (206) 757-7700
E-mail: steverummage@dwt.com
E-mail: fredburnside@dwt.com
E-mail: zanabugaighis@dwt.com

[7] Microsoft believes the Court can and should resolve this Motion for Summary Judgment before reaching the pending Motion for Class Certification, as summary judgment dismissing Ms. Cousineau's SCA claim would moot the class issue. *See, e.g., In re iPhone Application Litig.*, 2013 U.S. Dist. LEXIS 169220, *74 (N.D. Cal. 2013) (granting summary judgment on geolocation privacy claims and denying pending motion for class certification as moot).

Davis Wright Tremaine LLP
LAW OFFICES
Suite 2200 · 1201 Third Avenue
Seattle, Washington 98101-3045
(206) 622-3150 · Fax: (206) 757-7700

CERTIFICATE OF SERVICE

I hereby certify that on December 5, 2013, the foregoing *Microsoft's Motion for Summary Judgment* was electronically filed with the Clerk of the Court using the CM/ECF system which will send notification of such filing to all counsel of record who receive CM/ECF notification, and that the remaining parties (if any) shall be served in accordance with the Federal Rules of Civil Procedure.

DATED this 5th day of December, 2013.

DAVIS WRIGHT TREMAINE LLP
Attorneys for Def. Microsoft Corporation

By *s/ Stephen M. Rummage*
Stephen M. Rummage, WSBA #11168
1201 Third Avenue, Suite 2200
Seattle, Washington 98101-3045
Telephone: (206) 757-8136
Fax: (206) 757-7700
E-mail: steverummage@dwt.com

Davis Wright Tremaine LLP
LAW OFFICES
Suite 2200 · 1201 Third Avenue
Seattle, Washington 98101-3045
(206) 622-3150 · Fax: (206) 757-7700